Engage

Engage Web Access – Instructivo

Soluciones S.A.

28/05/2018

Contenido

Acerca de este documento

Destinatarios

Este documento está destinado a usuarios técnicos, con conocimientos avanzados en la implementación de procesos con **Engage Business Solution 5 o superiores.**

Compatibilidad

Las funciones aquí descriptas son compatibles con versiones 5.9.0.0 de Engage o Superiores.

Caducidad

Este documento caduca el día 31-12-2021. Una vez caducado, solicitar o acceder a una nueva versión del mismo.

Formas de autenticación.

El Agente Web Access soporta las mismas formas de acceso que el Agente Web estándar, pero agrega variantes que dan flexibilidad para informar el usuario o el proceso de inicio, las cuales pueden ser útiles cuando se necesita utilizar un único usuario genérico Engage para todos los usuarios nominales.

Estas variantes son la de Login Directo y la de Login Directo con auto-inicio y no son nuevas formas de acceso, sino que son una manera de ingresar a la ejecución de procesos, con un usuario Engage prefijado.

Las formas de autenticación son tres, y se utilizan de la siguiente manera:

1- Login estándar de Engage:

Es la autenticación estándar de Engage, en la cual, según la forma de acceso se muestra el formulario de login (UsuarioClave, Desarrollo, NT_UsuarioClave) o se ingresa directamente (NT). En cualquier caso, cada usuario físico necesita tener definido un usuario Engage para poder ingresar.

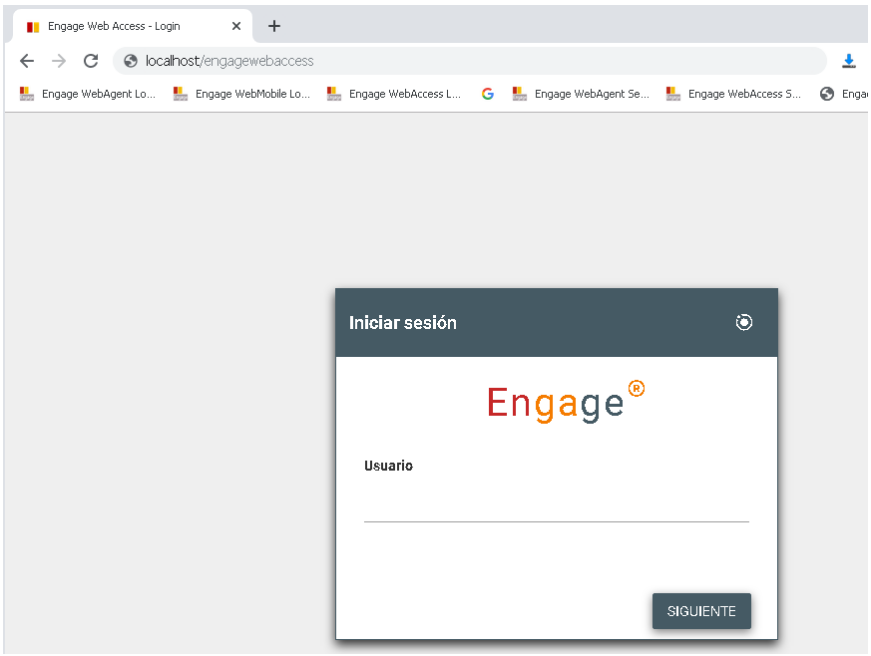
La url de login estándar del Web Access es la siguiente:

http://localhost/EngageWebAccess/

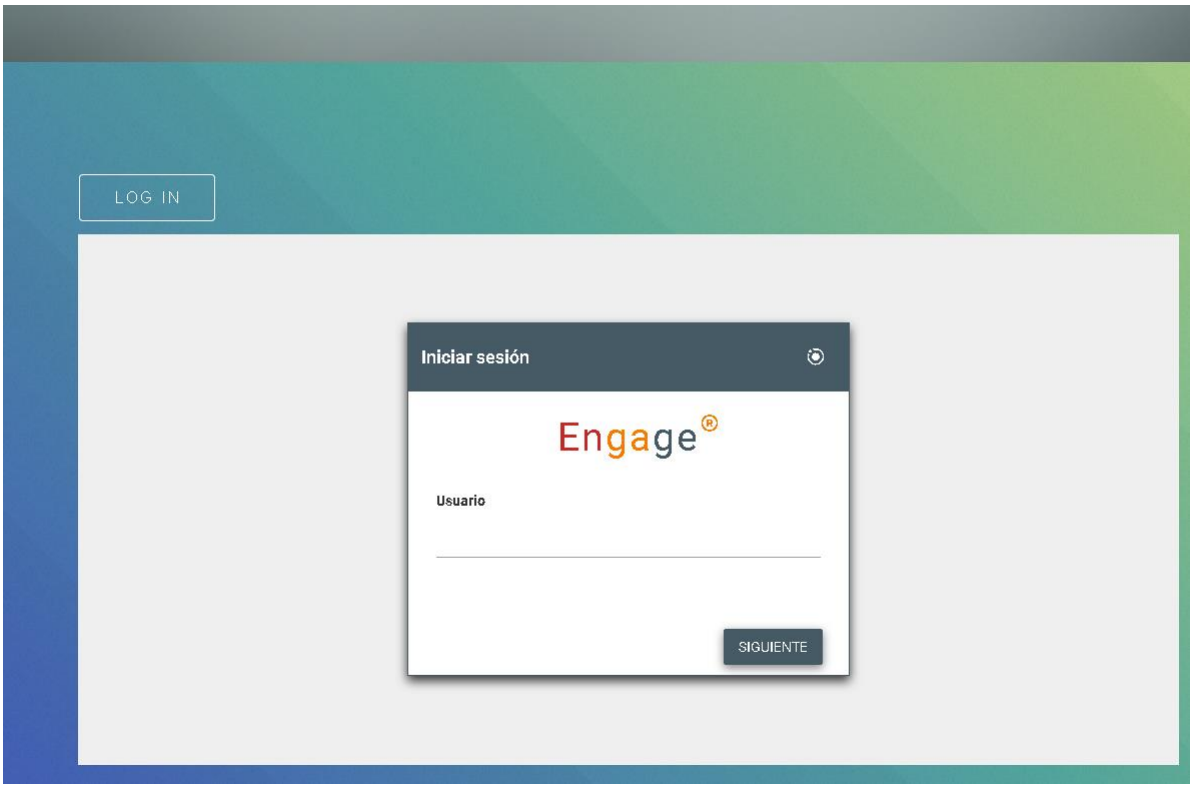
Siendo “EngageWebAccess” el nombre de la aplicación web definida en el IIS cuando se instaló WebAccess, ejemplo:

La URL puede invocarse directamente desde una ventana de un explorador, en un pop up o en un iframe:

Ejemplo de explorador/pop up:



Ejemplo de ejecución en un iframe de una página web:



Para que se pueda iniciar un proceso con esta forma de autenticación el proceso tiene que ser del tipo AUTOEJECUTABLE (AUTOEXEC). Ver el Anexo de este documento para tener información sobre los procesos del tipo AUTOEXEC.

2- Login directo:

Por las características del Agente Web Access, puede existir la necesidad de que todos los usuarios físicos ingresen con el mismo usuario Engage. De esta manera, no hará falta que cada usuario físico tenga definido su correspondiente usuario Engage para ingresar. Y además, tampoco se necesitará el formulario de login. Para poder utilizar el login directo, se debe utilizar la siguiente URL:

http://localhost/EngageWebAccess/Account/DirectLogin

Pero también se necesitan definir los siguientes parámetros de aplicación en el archivo web.config que de fábrica salen comentados:

```
<add key="DirectLoginUser" value="user1" />
<add key="DirectLoginUnit" value="UNIDADTEST" />
<add key="DirectLoginPassword" value="PLAIN:" />
```

Dónde: **DirectLoginUser** (obligatorio), es el ID del usuario Engage con el que se registraran todos los usuarios físicos que ingresen al Agente Web Access; **DirectLoginPassword** (opcional), sólo debe informarse si la forma de acceso definida en la tabla PRM admite clave, pudiendo incluirse en forma legible (con el prefijo "PLAIN:"), o encriptada con el utilitario EngageEncrypt; **DirectLoginUnit**: es la unidad en la que trabajará el usuario durante toda la sesión.

De esta manera, cuando se utilice esta URL se iniciara directamente el proceso al usuario y unidad definido en el web.config.

Para que se pueda iniciar un proceso con esta forma de autenticación el proceso tiene que ser del tipo AUTOEJECUTABLE (AUTOEXEC). Ver el Anexo de este documento para tener información sobre los procesos del tipo AUTOEXEC.

3- Login directo con auto-inicio:

Esta forma de autenticación tiene características similares al login directo, en cuanto a que permite ingresar con un usuario prefijado sin pasar por el formulario de login. La diferencia está en que el usuario y la unidad se pasan encriptados en un parámetro de la URL, en lugar de informarlos en el archivo web.config como se mencionó antes. Esto permite un manejo más flexible de los datos de ingreso, puesto que se pueden definir por cada invocación en lugar de globalmente para todas. Otra diferencia con respecto al login directo es que, además, se puede informar un proceso para iniciar o retomar a través del parámetro de entrada encriptado de la URL. Para poder utilizar el login directo, se debe utilizar la siguiente URL:

http://localhost/engagewebaccess/Account/DirectStartup?prm=<string_encriptado>

El parámetro prm=<string_encriptado> contiene los datos encriptados de la autenticación y del proceso de inicio. Pero para poder obtener dicho string, se debe enviar un mensaje a EngageIntegrationService a través de una transacción de socket utilizando el servicio UTILX de acuerdo a lo que se necesite (iniciar o retomar un trámite):

Mensajes posibles:

Para iniciar un proceso:
UTILX|GETSTARTACTIVITYSTARTUPPRM(UserId,UnitId,JobTypeCode,CustPkey,JobOriginPkey,Prm1=val1;Prm2=val2)[EOM]

Para retomar un proceso:
UTILX|GETRESTARTACTIVITYSTARTUPPRM(UserId,UnitId,JobPkey,AttPkey,JobOriginPkey,Prm1=val1;Prm2=val2)[EOM]

Los parámetros JobOriginPkey y Prm son opcionales.

Los parámetros Prm=val sirven para guardar valores en uno o varios campos de la entidad del trámite que se va a ejecutar. El formato es el siguiente: Campo1=valor1; Campo2=valor2; etc. Donde "Campo1" es el nombre del campo de la entidad del trámite que se iniciara/retomara y "valor1" es el valor que se le quiere guardar a dicho campo.

El comando GETRESTARTACTIVITYSTARTUPPRM tiene tres variantes para el parámetro AttPkey (Pkey de la tabla ATTENDED_CUSTOMER):

-La Pkey directa, por ejemplo aaae6f0a-1996-495e-bc6b-8713200ccbbb

-La Pkey con prefijo: PKEY=aaae6f0a-1996-495e-bc6b-8713200ccbbb

-El código de actividad: CALL_TYPE_CODE=TM_ACT_5

Los siguientes son dos ejemplos de mensajes para generar las URLS encriptadas de un START y un RESTART con CALL_TYPE_CODE:

UTILX|GETSTARTACTIVITYSTARTUPPRM(usuario1,DESA_PRUEBA,TEST_BATCH,0003916516_77,,ACTIVO=TRUE;DESCRIPCION=TEST;ESTADO=1)[EOM]

String Resultante:

H4sIAAAAAAAEAA3IS4JDMAAA0ANZqGlpLbooEt9SBImdafyGmdJqEk7fecsnw98G0yAthcLKUuQlVJCyM8M3tEOvH%2fQnfztoFBX%2fCcKwI04k86HzXNWb87zV2oNhIfFIhbFWUpH8DxsXA0HMd36cHO405hoOSX3vLtwqr81R37SNrLjfJ%2fxoejfXPab6pCQZ0Ydxvw5FWzxPpv3mURagG2fO0mmsY%2fgBIo%2ba1lr33wUjLoDSVXmJF1loB1CQZzuEAZrqexUt3uxbsyZPZIxV%2bzLL4u9L8UsTUIbTpYIJLwYdNM8ZZactd2zJmoGs16rlbxSOXG1lRA%2f8fP4A%2f27WMhgBAAA%3d

URL Final:

http://localhost/engagewebaccess/Account/DirectStartup?prm=H4sIAAAAAAAEAA3IS4JDMAAA0ANZqGlpLbooEt9SBImdafyGmdJqEk7fecsnw98G0yAthcLKUuQlVJCyM8M3tEOvH%2fQnfztoFBX%2fCcKwI04k86HzXNWb87zV2oNhIfFIhbFWUpH8DxsXA0HM

d36cHO405hoOSX3vLtwqr81R37SNrLjfJ%2fxoejfXPab6pCQZ0Ydxvw5FWzxPpv3mURagG2fO0mmsY%2fgBIo%2ba1lr33wUjLoDSVXmJF1loB1CQZzuEAZrqexUt3uxbsyZPZIxV%2bzLL4u9L8UsTUIbTpYIJLwYdNM8ZZactd2zJmoGs16rlbxSOXG1lRA%2f8fP4A%2f27WMhgBAAA%3d

Cuando se ejecute esta URL, se iniciara automáticamente el proceso "TEST_BATCH" con el usuario "USUARIO1" y la unidad "DESA_PRUEBA" en el agente Web Access, sin pasar por la pantalla de Login.

UTILX|GETRESTARTACTIVITYSTARTUPPRM(USUARIO1,DESA_PRUEBA,a18e6f0a-1996-495e-bc6b-8713200cc07b,CALL_TYPE_CODE=TM_ACT_5)[EOM]

String Resultante:

H4sIAAAAAAAEAAXB0RZCMBgA4Ady4QzJLhuKwxgip7smoZQY%2fuXp%2b77PwlHbpFQSsqqmN%2ftFR19GNpg4%2fLGIa%2fsnClv1WlYH4BEHJn582lSWIfJaN2E1TQwOqvK8GQR9uEkmz%2fr3M95ypDg0N4yowPOB%2bVOCSz9Iei4Gn2QRNqVDaM0qctFcLwVsqeJRdovem7G%2bA3ivTrxVYZFCDffTqpGRLHx%2fXJQ%2bsJ%2bKbIdkxqMF2N7Vf%2bHF8DDAAAAA

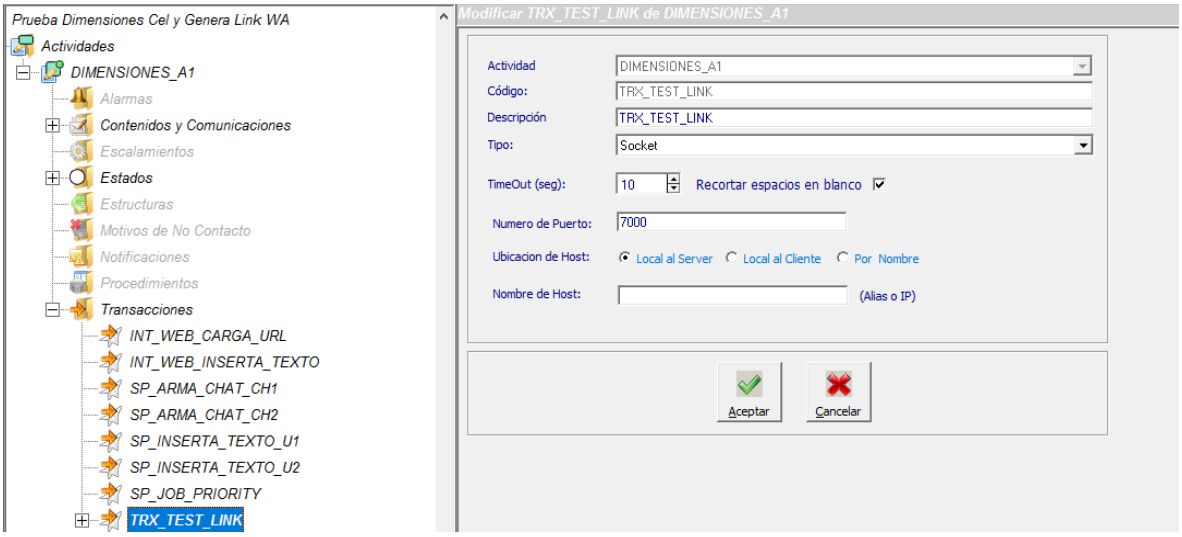
URL Final:

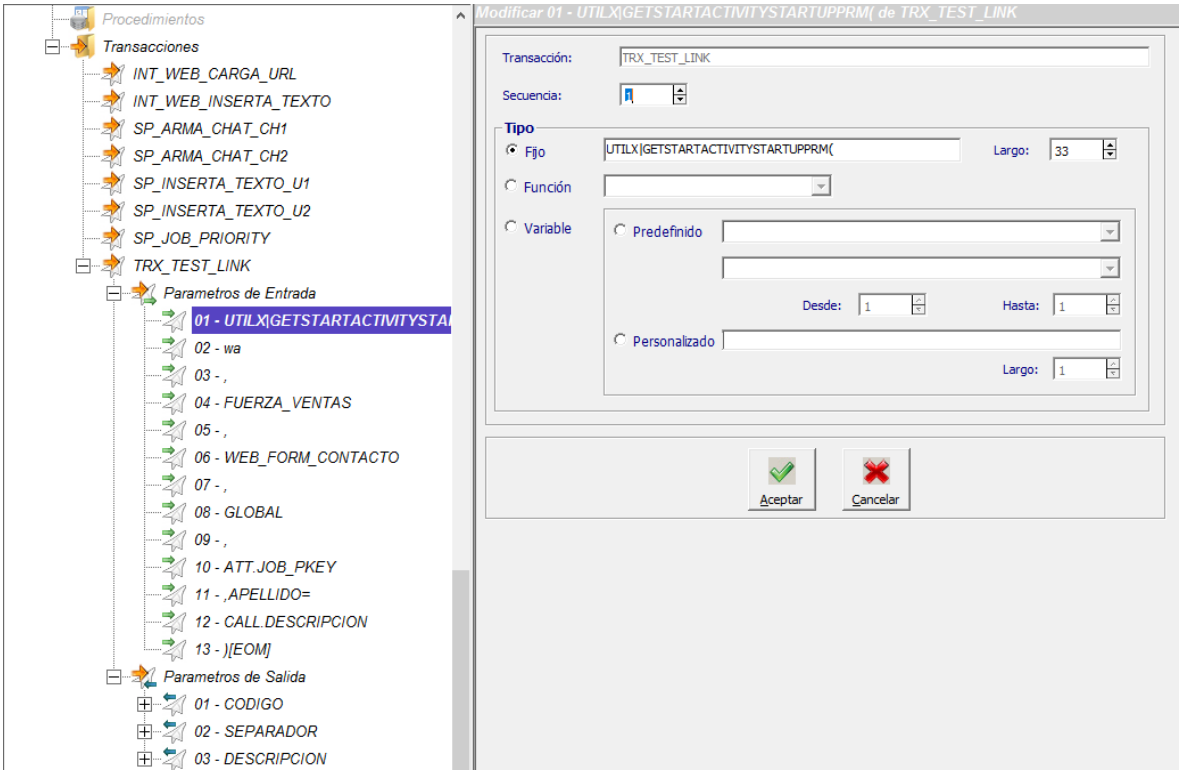
http://localhost/engagewebaccess/Account/DirectStartup?prm=H4sIAAAAAAAEAAXB0RZCMBgA4Ady4QzJLhuKwxgip7smoZQY%2fuXp%2b77PwlHbpFQSsqqmN%2ftFR19GNpg4%2fLGIa%2fsnClv1WlYH4BEHJn582lSWIfJaN2E1TQwOqvK8GQR9uEkmz%2fr3M95ypDg0N4yowPOB%2bVOCSz9Iei4Gn2QRNqVDaM0qctFcLwVsqeJRdovem7G%2bA3ivTrxVYZFCDffTqpGRLHx%2fXJQ%2bsJ%2bKbIdkxqMF2N7Vf%2bHF8DDAAAAA

Cuando se ejecute esta URL, se retomara automáticamente el proceso con la jobpkey y attpkey indicada en el mensaje con el usuario "USUARIO1" y la unidad "DESA_PRUEBA" en el agente Web Access, sin pasar por la pantalla de Login.

Ejemplo de transacción de socket para generar el parámetro encriptado:

Para iniciar un proceso:





Siendo:

wa: el usuario con el que se iniciara el proceso al ejecutar la URL. Puede ser un usuario anónimo o genérico.

FUERZA_VENTAS: la unidad con la que se iniciara el proceso al ejecutar la URL.

WEB_FORM_CONTACTO: el código del proceso que se iniciara al ejecutar la URL.

GLOBAL: La pkey del cliente al que se le iniciara el proceso al ejecutar la URL.

ATT.JOB_PKEY: Pkey del proceso padre del que se iniciara al ejecutar la URL (opcional).

APELLIDO=CALL.DESCRIPCION: Este parámetro indica que se guardara en el campo APELLIDO de la entidad principal del trámite que se iniciara en el Web Access, el valor del campo "Descripción" de la entidad principal del trámite que ejecutara la transacción de socket (opcional).

Parámetros de Salida:

CODIGO VARCHAR(5)
SEPARADOR VARCHAR(1)
DESCRIPCION VARCHAR(2000)

Como respuesta, la transacción de socket devolverá un string encriptado similar al siguiente: "H4sIAAAAAAAAEAA3IS4JDMAAA0ANZqGlpLbooEt9SBImdafyGmdJqEk7fecsnw98G0yAthcLKUuQlVJCyM8M3tEOvH%2fQnfztoFBX%2fCcKwI04k86HzXNWb87zV2oNhIfFIhbFWUpH8DxsXA0HMd36cHO405hoOSX3vLtwqr81R37SNrLjfJ%2fxoejfXPab6pCQZ0Ydxvw5FWzxPpv3mURagG2fO0mmsY%2fgBIo%2ba1lr33wUjLoDSVXmJF1loB1CQZzuEAZrqexUt3uxbsyZPZIxV%2bzLL4u9L8UsTUIbTpYIJLwYdNM8ZZactd2zJmoGs16rlbxSOXG1lRA%2f8fP4A%2f27WMhgBAAA%3d"

Dicho string será devuelto en el parámetro de salida "DESCRIPCION" de la transacción de socket.

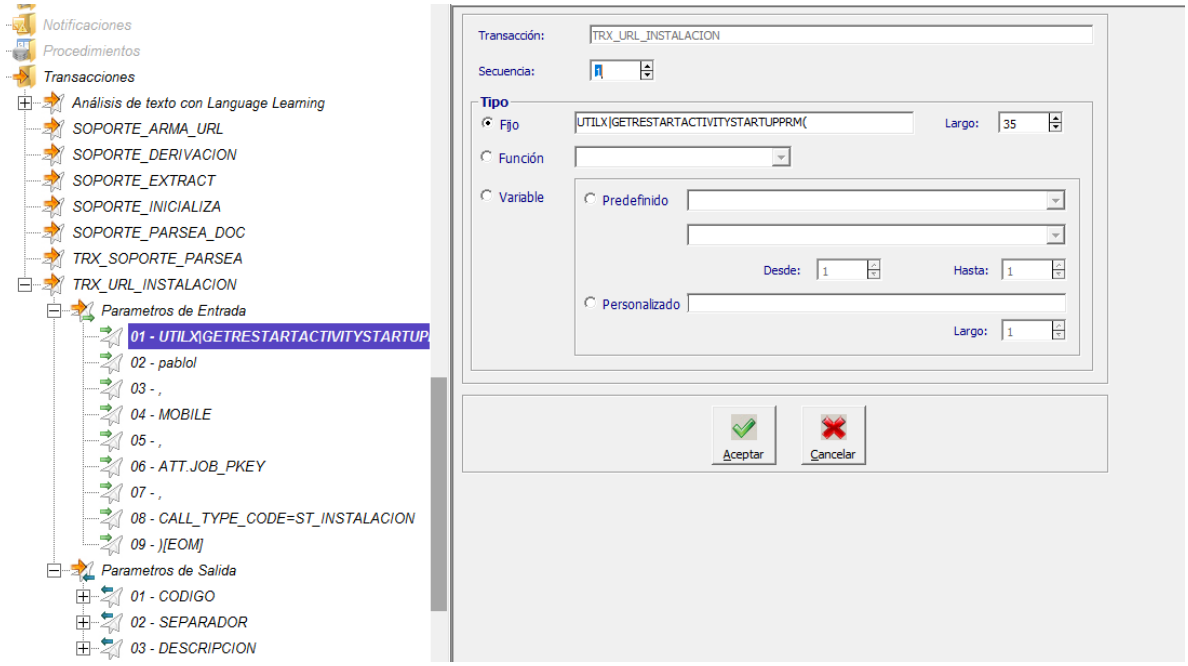
Que deberá enviarse como parámetro en la URL del web Access tal como se mencionó anteriormente, quedando la url final, conformada de la siguiente forma:

http://localhost/engagewebaccess/Account/DirectStartup?prm=H4sIAAAAAAAAEAA3IS4JDMAAA0ANZqGlpLbooEt9SBImdafyGmdJqEk7fecsnw98G0yAthcLKUuQlVJCyM8M3tEOvH%2fQnfztoFBX%2fCcKwI04k86HzXNWb87zV2oNhIfFIhbFWUpH8DxsXA0HMd36cHO405hoOSX3vLtwqr81R37SNrLjfJ%2fxoejfXPab6pCQZ0Ydxvw5FWzxPpv3mURagG2fO0mmsY%2fgBIo%2ba1lr33wUjLoDSVXmJF1loB1CQZzuEAZrqexUt3uxbsyZPZIxV%2bzLL4u9L8UsTUIbTpYIJLwYdNM8ZZactd2zJmoGs16rlbxSOXG1lRA%2f8fP4A%2f27WMhgBAAA%3d

Entonces al hacer click en esta URL o incluirla dentro de un iframe, se iniciara automáticamente el proceso en el agente Web Access.

Ejemplo de transacción de socket para generar el parámetro encriptado:

Para retomar un proceso:



Siendo:

pablol: el usuario con el que se retomará el proceso al ejecutar la URL.

MOBILE: la unidad con la que se retomará el proceso al ejecutar la URL.

ATT.JOB_PKEY: La pkey del proceso que se retomará.

CALL_TYPE_CODE=ST_INSTALACION: el código de la actividad en la que se retomará el proceso.

En este caso no se utiliza la JobOriginPkey ni los Prm para pasarle valores a la entidad del trámite.

Como respuesta, la transacción de socket devolverá un string encriptado que deberá enviarse como parámetro en la URL del web Access tal como se mencionó anteriormente, quedando la url final, conformada de la siguiente forma:

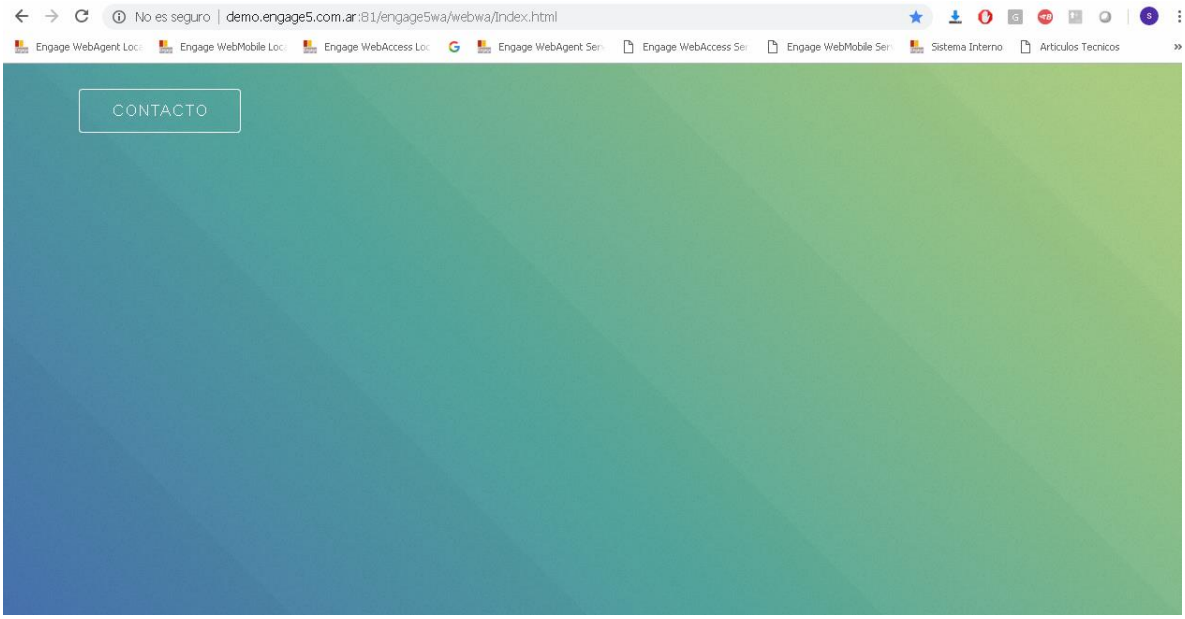
http://localhost/engagewebaccess/Account/DirectStartup?prm=H4sIAAAAAAAEAAXB0RZCMBgA4Ady4QzJLhuKwxgip7smoZQY%2fuXp%2b77PwlHbpFQSsqqmN%2ftFR19GNpg4%2fLGIa%2fsnClv1WlYH4BEHJn582lSWIfJaN2E1TQwOqvK8GQR9uEkmz%2fr3M95ypDg0N4yowPOB%2bVOCSz9Iei4Gn2QRNqVDaM0qctFcLwVsqeJRdovem7G%2bA3ivTrxVYZFCDffTqpGRLHx%2fXJQ%2bsJ%2bKbIdkxqMF2N7Vf%2bHF8DDAAAAA

Entonces al hacer click en esta URL o incluirla dentro de un iframe, se retomará automáticamente el proceso en el agente Web Access.

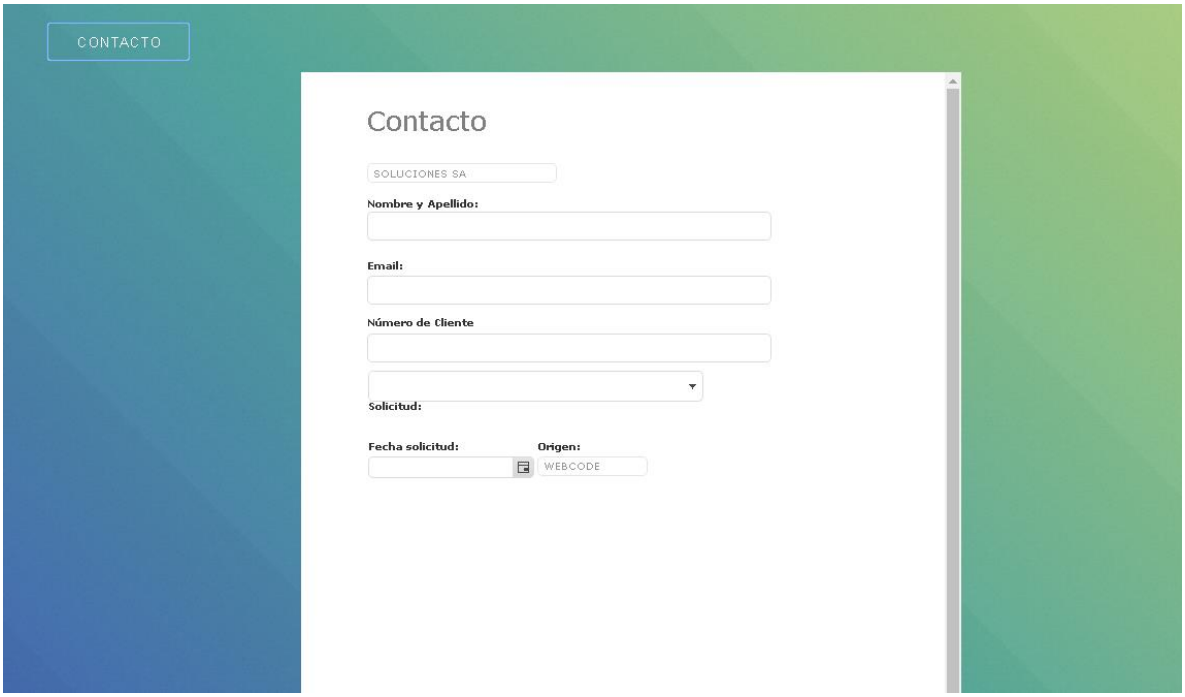
Ejemplos de uso del link generado con login directo con autoinicio:

Dentro de una página web en un iframe:

Una vez generado el link cifrado siguiendo los pasos explicados anteriormente, puede incluirse dicho link para que se ejecute en un iframe de una página web, por ejemplo al presionar un botón:

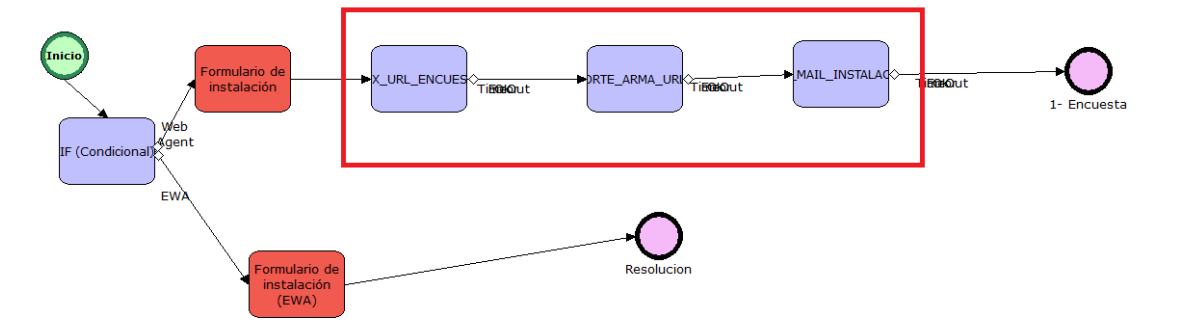


Se presiona el botón “Contacto” y en un iframe se ejecuta el link de web Access con el string encriptado para que se inicie automaticamente el proceso sin pasar por el login:



Enviar un email con link a Web Access:

Para enviar un email a un cliente con un link que cuando sea presionado se inicie o retome un trámite en Web Access se necesitan ejecutar tres pasos encadenados en Designer: Dos transacciones de socket y un SP, tal como se ve en el recuadro rojo de la siguiente imagen:



El primero de los tres pasos es una transacción de socket que invoca al comando UTILX para generar el link encriptado, tal como se explicó en la sección “Ejemplo de transacción de socket para generar el parámetro encriptado” anteriormente en este documento. Una vez ejecutada esta transacción de socket, nos devolverá en el parámetro de salida “DESCRIPCION” el link cifrado, que se utilizará en el SP que sigue a continuación.

Tener en cuenta que la generación del link cifrado puede realizarse tanto para iniciar como para retomar un proceso en WebAccess (ver sección “3- Login directo con autoinicio” de este documento).

El segundo paso es un SP que se encarga de guardar en una variable, el código HTML para generar un link que al presionarlo ejecute una URL. Esto se puede hacer por ejemplo con el siguiente código SQL:

```
SET @URL1='http://localhost/engagewebaccess/Account/DirectStartup?prm=' + ISNULL(@PRM,'')

SET @URL2='<a href="'+ISNULL(@URL1,'')+'"><span>Encuesta de Satisfacción</span></a>'
```

Donde @PRM contiene lo que devolvió la transacción de socket ejecutada en primer paso y que encriptó los parámetros.

Y luego guardar esa variable armada en el SP en un campo de la entidad principal del trámite (ejemplo TMT_SOPORTE):

```
UPDATE TMT_SOPORTE
SET LINK_ENCUESTA=@URL2
WHERE PAR_KEY=@PKEY_JOB
```

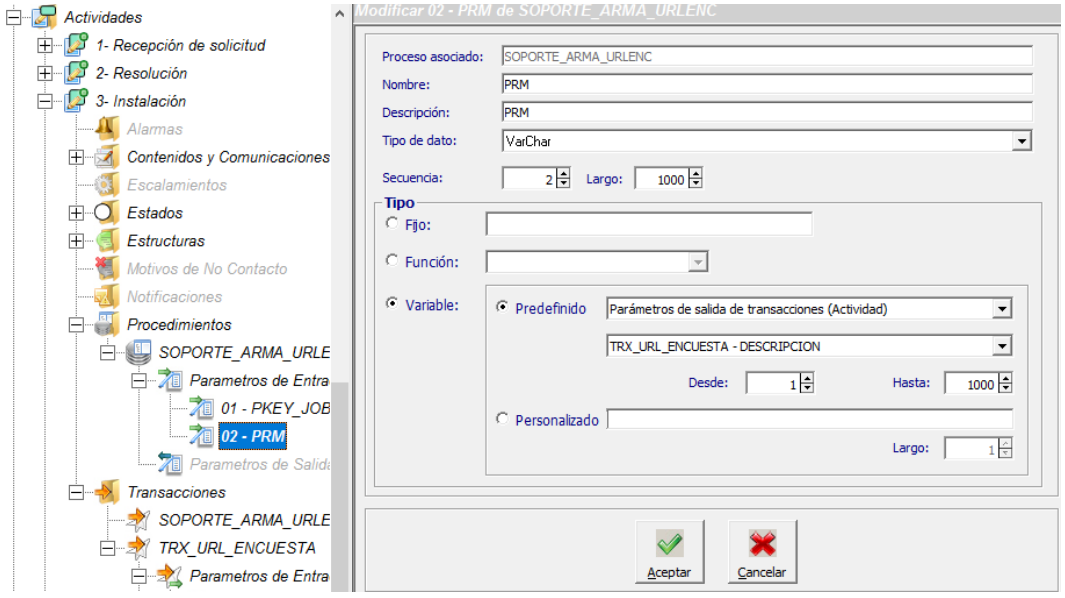
Nota: En la variable @URL1 se guarda la URL del Web Access con los parámetros del login directo con autoinicio encriptados incluidos.
En la variable @URL2 se guarda el código HTML para generar un link que al presionarlo abra en una ventana la URL guardada en la variable @URL1.

Ejemplo de un SP que ejecuta el código anterior:

```
ALTER procedure [dbo].[SOPORTE_ARMA_URLENC]
@PKEY_JOB VARCHAR(100),
@PRM VARCHAR(1000)
AS

BEGIN

DECLARE @URL1 VARCHAR(4000),
@URL2 VARCHAR(4000)

SET @URL1='http://localhost/engagewebaccess/Account/DirectStartup?prm=' + ISNULL(@PRM,'')

SET @URL2='<a href="'+ISNULL(@URL1,'')+'"><span>Encuesta de Satisfacción</span></a>'

UPDATE TMT_SOPORTE
SET LINK_ENCUESTA=@URL2
WHERE PAR_KEY=@PKEY_JOB

END
```

Nota: En el SP, se deberá modificar “localhost” por la IP del servidor correspondiente donde se encuentra instalado el Web Access.

Tal como se ve en la imagen anterior, el parámetro “PRM” es un parámetro de entrada del SP que recibe como entrada la encriptación que devolvió la transacción de socket del paso anterior, en el parámetro de salida “DESCRIPCION”, tal como se puede ver en la siguiente imagen:



Donde TRX_URL_ENCUESTA es la transacción de socket del primer paso.

Entonces, en el flujo del proceso en Designer, se ejecutaría primero la transacción de socket que invoca al servicio UTILX para generar el link encriptado (ya sea para iniciar o retomar un proceso) y luego el SP que toma lo que devolvió la transacción y arma el link para invocar a Web Access y el HTML para que al presionarlo se ejecute dicho link.

Por último se ejecuta el tercer paso, que es una transacción de socket para enviar emails a través de EngageIntegrationService.

La documentación para el envío de emails a través de EIS se encuentra en el siguiente link:

https://services.engage-sc.com.ar/manuales-y-documentos/engage-5-envio-de-emails/

Para que en el email se envíe el HTML generado en el SP del segundo paso se deberá armar un formato de envío de emails (template) que contenga el reemplazo del campo de la entidad del trámite donde se guardó dicho HTML, en este caso de ejemplo, se guardó en el campo "LINK_ENCUESTA" de la entidad "TMT_SOPORTE", entonces el reemplazo del campo en el template quedaría de la siguiente forma:

<ENG_TMT_SOPORTE.LINK_ENCUESTA>

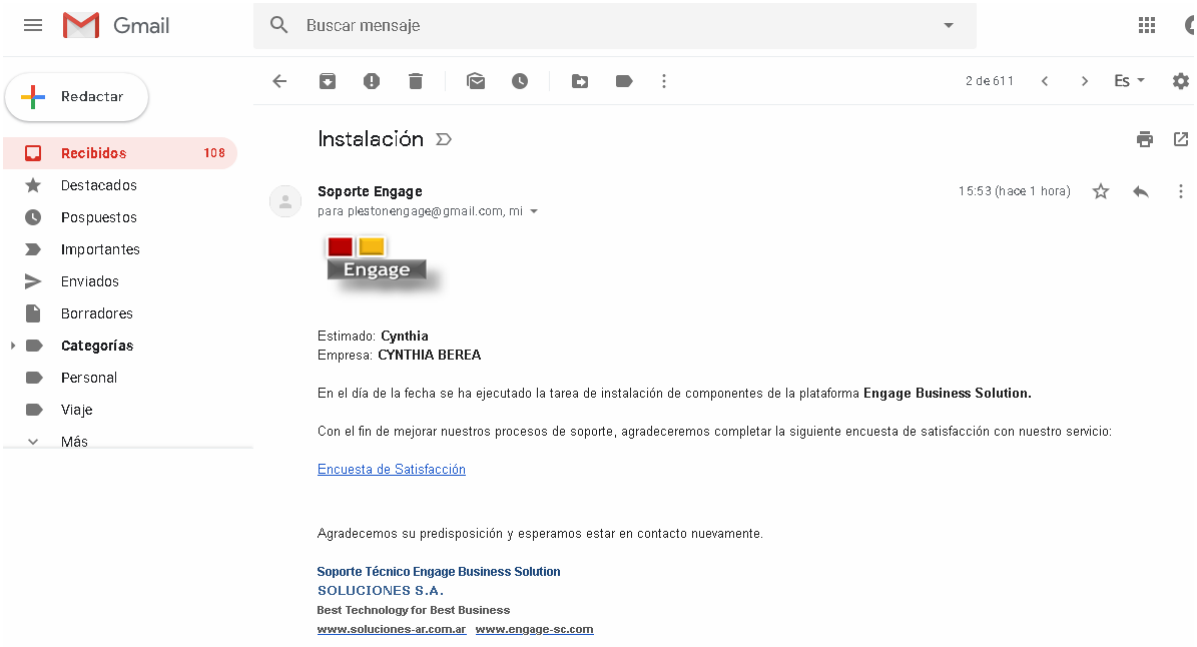
En la siguiente imagen se puede ver un ejemplo del código HTML del template utilizado en este caso:

```
<body lang=ES-AR>

<div class=WordSection1>

<p class=MsoNormal><img width=132 height=73 id="Imagen 2"
src="Instalacion_archivos/image001.png"></p>
<br>

<p class=MsoNormal>Estimado: <B><ENG_CS_DATOS_CLIENTE.CONTACTO_PRINCIPAL></B></p>

<p class=MsoNormal>Empresa: <B><ENG_CUSTOMER.CUSTOMER_NAME></B></p>
<br>

<p class=MsoNormal>En el día de la fecha se ha ejecutado la tarea de
instalación de componentes de la plataforma <b>Engage Business Solution.</b></p>

<p class=MsoNormal> </p>

<p class=MsoNormal>Con el fin de mejorar nuestros procesos de soporte, agradeceremos
completar la siguiente encuesta de satisfacción con nuestro servicio:</p>
<br>

<p class=MsoNormal><ENG_TMT_SOPORTE.LINK_ENCUESTA></p>

<br>
<p class=MsoNormal>Agradecemos su predisposición y esperamos estar en contacto
nuevamente.</p>
```

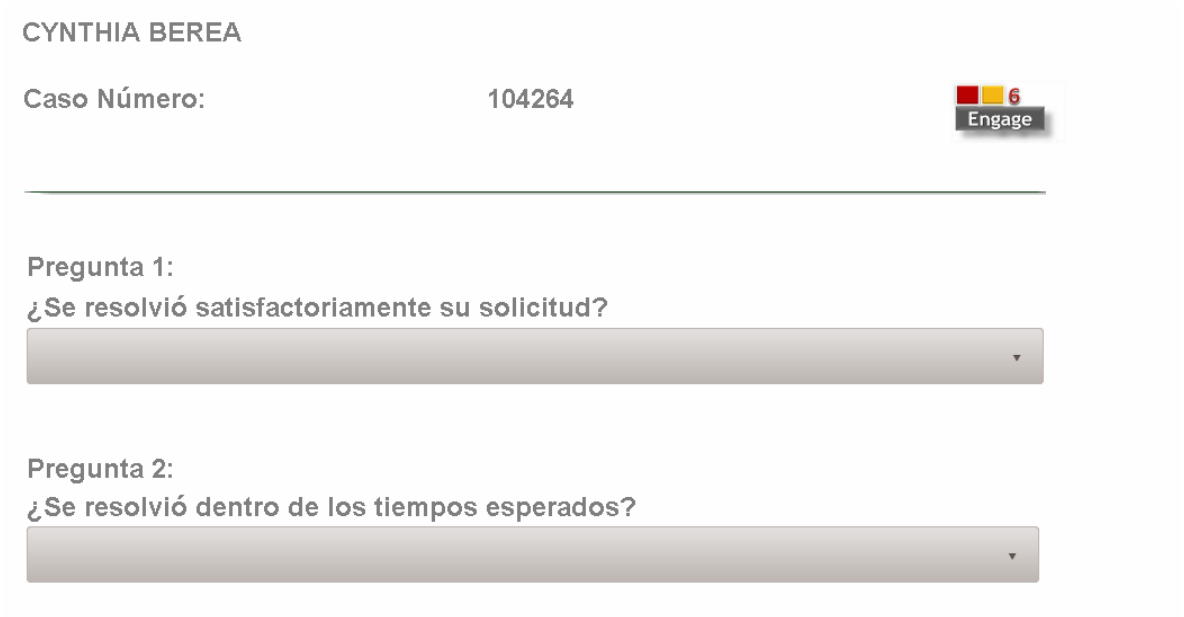
Entonces cuando al usuario le llegue el mail, vera el link en el lugar que se utilizó el reemplazo y al hacer click se iniciará/retomará el proceso con el usuario y todos los datos que se hayan definido en la transacción de socket.

Ejemplo:

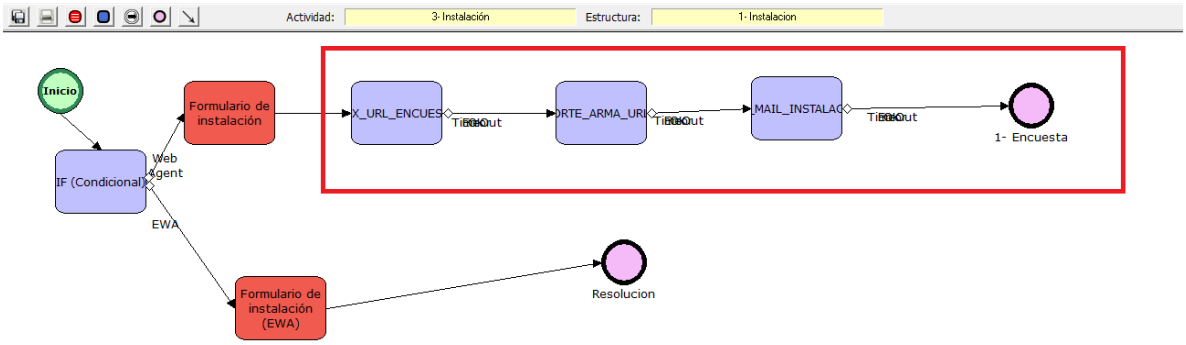
Mail enviado con el Link a Web Access:

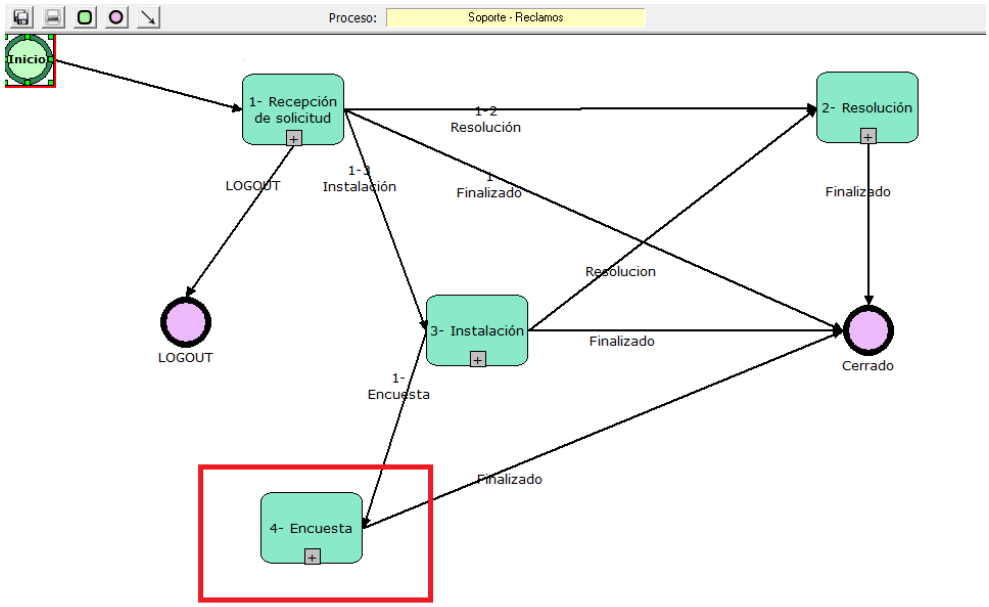


Al hacer click sobre el Link generado en el SP “Encuesta de Satisfacción”, automáticamente se abre en una nueva ventana el Web Access y se inicia/retoma un proceso de acuerdo a los datos que se configuraron en la transacción de socket:



Nota: En caso de que hayan generado un link encriptado para iniciar o retomar un proceso distinto, alcanzaría con los tres pasos mencionados anteriormente, pero en el caso que necesiten que el link retome el mismo trámite desde el cual se generó y se envió el email (pero en otra actividad), lo que se debe hacer luego del tercer paso (el envío del email) es derivar el tramite a otra actividad, y al generar el link, utilizar el CALL_TYPE_CODE (en vez de la PKEY) de la actividad no trabajada a la que se derivó (tal como el ejemplo que se encuentra en la sección "3- Login directo con autoinicio" de este documento) para que cuando se ejecute el link enviado por mail, se retome el trámite en la nueva actividad a la que se lo derivo. Por ejemplo, en el flujo de la imagen que vimos anteriormente (que se encuentra en la actividad "Instalación"), luego de los tres pasos mencionados se deriva el trámite a la actividad "Encuesta":





Como se ve en las imágenes anteriores, luego de generar el link cifrado con la transacción de socket, armar el HTML con el SP y enviar el email, se deriva el tramite a la actividad “Encuesta” (que va a estar como no trabajada) hasta que el cliente presione el link del email y retome el trámite en dicha actividad.

En caso de que el link generado sea para iniciar o retomar un proceso distinto, no sería necesaria esta derivación.

Procesos AUTOEXEC:

La interface del Agente Web Access es principalmente un contenedor donde se ejecuta un único proceso, con lo cual, no hay forma de utilizar la Inbox o la Búsqueda de Clientes para seleccionar el proceso que se quiere iniciar o retomar. Dado lo anterior, y a menos que se utilice la forma de autenticación de login directo con autoinicio (la cual tiene prioridad), al iniciar el Agente Web Access se invoca a un tipo de proceso automático llamado AUTOEXEC.

1- Características y condiciones:

Un proceso AUTOEXEC debe ser siempre un proceso GLOBAL. Los procesos AUTOEXEC no se muestran en la Inbox ni en la Historia del Agente Web estándar. Como cualquier otro proceso, deben asignarse los permisos correspondientes y debe estar vigente para que los usuarios puedan ejecutarlo. Un proceso AUTOEXEC se inicia por decreto con el cliente GLOBAL. Al diseñar un proceso AUTOEXEC, es recomendable que siempre finalice en un estado de cierre.

2- Nomenclatura:

Para saber qué proceso es de tipo AUTOEXEC, se utiliza siempre el prefijo AUTOEXEC en el código del tipo de proceso. Y para saber cuándo debe ejecutarse, se usa un sufijo variable que debe coincidir con el ID de usuario, el ID de una unidad o la constante GLOBAL. Por ejemplo:

AUTOEXEC_USUARIO1: Este proceso se ejecutará sólo cuando el usuario USUARIO1 ingresa al Agente Web Access.

AUTOEXEC_DESARROLLO: Este proceso se ejecutará cuando cualquier usuario ingrese al Agente Web Access con la unidad DESARROLLO.

AUTOEXEC_GLOBAL: Este proceso se ejecutará cuando cualquier usuario ingrese al Agente Web Access.

Es posible que más de un proceso coincida para un usuario que se acaba de registrar. En ese caso, la precedencia es siempre: usuario, unidad, global. Es decir, de lo más específico a lo más genérico.

Nota: El Agente Web estándar también soporta procesos AUTOEXEC, con lo cual, si se utiliza un proceso demasiado abarcativo (por ejemplo, AUTOEXEC_GLOBAL), se puede generar un comportamiento no deseado.

3- Forma de instanciación:

Cuando un usuario ingresa al Agente Web Access, si ya existía un proceso AUTOEXEC abierto para la combinación usuario-unidad, entonces se retoma ese proceso. En caso contrario, se inicia uno nuevo en forma automática. Sin embargo, hay una excepción cuando se utiliza un login directo. En este caso, dado que muchos usuarios físicos ingresarán con el mismo usuario Engage, habrá una altísima probabilidad de que se produzcan conflictos por acceder a la misma instancia del proceso en forma concurrente. Por ello, cuando se utiliza un login directo se fuerza siempre al inicio de una nueva instancia del proceso AUTOEXEC.

Nota: Esta forma de instanciación de los procesos AUTOEXEC (cuando existe se retoma y cuando no existe se inicia), está pensada para evitar innumerables instancias del proceso. Sin embargo, este método no garantiza que todos los procesos AUTOEXEC se cierren siempre, con lo cual, se recomienda efectuar un control para cerrar y/o depurar procesos AUTOEXEC.